Quantum key distribution with triggering parametric down conversion sources

Xiongfeng Ma[1,*] and Hoi-Kwong Lo[1,†]

[1]*Center for Quantum Information and Quantum Control, Department of Electrical & Computer Engineering and Department of Physics, University of Toronto, Toronto, Ontario, Canada, M5S 1A7*

Abstract

Parametric down-conversion (PDC) sources can be used for quantum key distribution (QKD). One can use a PDC source as a triggered single photon source. Recently, there are various practical proposals of the decoy state QKD with triggering PDC sources. In this paper, we generalize the passive decoy state idea, originally proposed by Mauerer and Silberhorn. The generalized passive decoy state idea can be applied to cases where either threshold detectors or photon number resolving detectors are used. The decoy state protocol proposed by Adachi, Yamamoto, Koashi and Imoto (AYKI) can be treated as a special case of the generalized passive decoy state method. By simulating a recent PDC experiment, we compare various practical decoy state protocols with the infinite decoy protocol and also compare the cases using threshold detectors and photon-number resolving detectors. Our simulation result shows that with the AYKI protocol, one can achieve a key generation rate that is close to the theoretical limit of infinite decoy protocol. Furthermore, our simulation result shows that a photon-number resolving detector appears to be not very useful for improving QKD performance in this case. Although our analysis is focused on the QKD with PDC sources, we emphasize that it can also be applied to other QKD setups with triggered single photon sources.

PACS numbers:

*Electronic address: xima@physics.utoronto.ca

†Electronic address: hklo@comm.utoronto.ca

I. INTRODUCTION

Quantum key distribution (QKD) [1, 2] allows two legitimate parties, Alice and Bob, to create a random secret key even when the channel is accessible to an eavesdropper, Eve. The security of QKD is built on the fundamental laws of physics in contrast to existing classical public key encryption schemes that are based on unproven computational assumptions. Bennett and Brassard proposed a best-known protocol — BB84 [1]. Proving the security of QKD is a hard problem. Fortunately, this problem has been solved in the last decade, see for example, [3, 4, 5, 6]. Many security proofs are based on the assumption of idealized QKD system components, such as a perfect single photon source and well-characterized detectors. In practice, inevitable device imperfections may compromise the security unless these imperfections are well investigated. Meanwhile, the security of QKD with realistic devices has been proven. See [7, 8, 9, 10, 11, 12] for example.

In the original proposal of BB84 protocol, a single photon source is used. Unfortunately, single photon sources are still not commercially available with current technology. Alternatively, a weak coherent state is widely used as a photon source. We call this implementation *coherent state QKD*. Many coherent state QKD experiments have been done since the first QKD experiment [13].

The coherent state QKD suffers from photon-number splitting (PNS) attacks [9, 14, 15]. Nevertheless, it has been proven unconditionally secure by Inamori, Lütkenhaus and Mayers [10]. This work is improved by Gottesman, Lo, Lütkenhaus, and Preskill (GLLP) [12], though the performance in terms of the achievable secure distance and the key rate is limited.

Decoy state method [16] has been proposed to improve the performance of the coherent state QKD. The security of QKD with decoy states has been proven [17, 18, 19]. The simulation result shows us that the coherent state QKD with decoy states is able to operate as good as QKD with perfect single photon sources in the sense that the key generation rates given by both setups depend linearly on the channel transmittance [19]. Afterwards, some practical decoy-state protocols with only one or two decoy states are proposed [20], see also [21, 22, 23]. The experimental demonstrations for decoy state method have been done recently [24, 25, 26, 27, 28, 29].

The motivation of decoy states is to estimate the channel properties (e.g., transmittance

and error proability) better. To do that, Alice uses extra states with different light intensities during key transmission. Then Alice and Bob can consider detection statistics from signal and decoy states separately, from which they can estimate the channel transmittance and error probability better. We call the situation when Alice actively prepare decoy states *active decoy state* method to differentiate from the *passive decoy state* method where Alice choose decoy and signal states by passive measurements. Details can be found in Section IV. We note that in coherent state QKD, one can only use active decoy state method.

Other than the decoy state method, we remark that there are other approaches to enhance the performance of the coherent state QKD, such as QKD with strong reference pulses [30, 31] and differential-phase-shift QKD [32].

Besides a coherent state source, a parametric down-conversion (PDC) source can be used for QKD as well. There are two ways to use a PDC source for QKD. The first is to use it as a triggered (heralded) single photon source. Alice detects one of the two modes from a PDC source as a trigger [47] and actively encodes her qubit information into another mode. We call this implementation *triggering PDC QKD*. The second way is to use it as an entangled photon source for entanglement-based QKD protocols. See Ref. [33] and references cited therein. We call this implementation *entanglement PDC QKD*.

The triggering PDC QKD, similar to the coherent state QKD, suffers from PNS attacks. By applying the GLLP security proof, one can find that the optimal average photon number μ is in the same order of overall transmittance η. Then the key generation rate will be on the order of η^2. For a rigorous derivation, one can refer to Appendix A. Thus, the performance of the triggering PDC QKD is very limited.

Since decoy states idea can substantially enhance the performance of the coherent state QKD, a natural question will be: "can decoy states idea be applied to the triggering PDC QKD?" The answer is *yes*. One can apply the infinite decoy state idea [19] to the triggering PDC QKD. Not surprisingly, with decoy states, the key generation rate can be $O(\eta)$, which is the same as the order achieved by a single-photon source. Therefore, we expect the decoy state QKD to become a standard technique not only in the coherent state QKD, but also in QKD with triggering PDC sources. The infinite decoy state protocol requires an infinite number of decoy states to be used, which is not practical. A few practical decoy proposals for triggering PDC requiring a finite number of decoy states have been proposed [34, 35, 36, 37].

We are interested in comparing various protocols for the triggering PDC QKD. Among

the practical decoy protocols for triggering PDC QKD, we find that the one proposed by Adachi, Yamamoto, Koashi and Imoto (AYKI) [35] is simple to implement. The AYKI protocol is conceptually similar to the one-decoy-state scheme [20]. In the AYKI protocol, Alice and Bob only need to consider the statistics of triggered and non-triggered detection events [48] separately, instead of preparing new signals for decoy states. We emphasize that the AYKI protocol is easy to implement since there is no need for a hardware change.

Other decoy state proposals for the triggering PDC QKD require hardware modifications. For example, the one proposed by Mauerer and Silberhorn [34] requires photon-number resolving detectors, and the one proposed by Wang, Wang and Guo [36] requires Alice's pumping the laser source at various intensities.

We generalize the passive decoy state idea proposed by Mauerer and Silberhorn [34]. The main idea is that, Bob can group his detection events according to the public announcement of Alice's detection events. For example, when Alice uses a threshold detector, Bob can group his detection results according to whether Alice gets a detection or not. The generalized passive decoy state idea can be applied to both cases of using threshold detectors and photon-number resolving detectors. The AYKI protocol can be treated as a special case of the generalized passive decoy state protocol.

By simulating a recent PDC experiment [38], we compare one case with a perfect photon-number resolving detector and four cases with threshold detectors: no decoy, infinite decoy, weak decoy and AYKI. Our simulation result shows that in a large parameter regime, the performance of AYKI protocol is close to that of the infinite decoy protocol and thus there is not much room left for improvement after the AYKI protocol has been implemented. Also, the QKD performance of the case with the infinite decoy protocol using threshold detectors is close to the case using a perfect photon-number resolving detector. Thus, a photon-number resolving detector appears to be not very useful for triggering PDC QKD.

We emphasize that one advantage of passive decoy state method is that by passively choosing decoy and signal states, the possibility that Eve can distinguish decoy and signal states is reduced. On the other hand, in active (regular) decoy state experiments, it is more difficult to verify the assumption that Eve cannot distinguish decoy and signal states.

We note that the passive decoy state idea can be combined to the active decoy state idea. In Ref. [37], the authors gave a special case of combining passive and active decoy state ideas. Note that for coherent state QKD, one can only use active decoy state methods.

Although our analysis is focussed on the QKD with PDC source, we emphasize that it can also be applied to QKD setups with other triggered single photon sources.

In Section II, we will review the experiment setup of the triggering PDC QKD. In Section III, we give a model for the triggering PDC QKD. In Section IV, we will study various post-processing schemes for the triggering PDC QKD. In Section V, we will compare various schemes of the triggering PDC QKD: non-decoy+threshold detectors, infinite decoy+threshold detectors, AYKI and the case with a perfect photon-number resolving detector, by simulating a real PDC experiment. In Appendix A, we consider the optimal PDC source intensities for the triggering PDC QKD.

II. EXPERIMENT SETUP

In triggering PDC QKD, a PDC source is used as a triggered single photon source [49]. The schematic diagram is shown in FIG. 1.

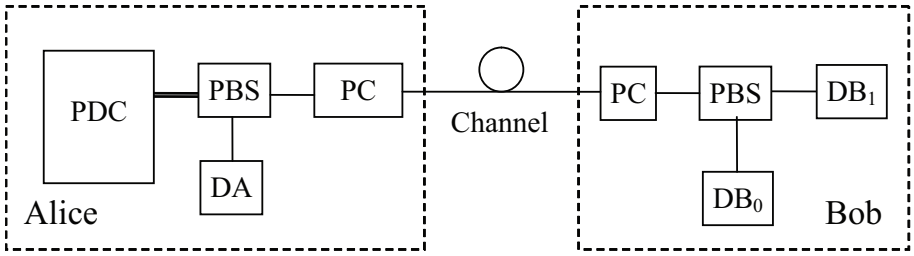

FIG. 1: A schematic diagram for the triggering PDC QKD. Alice collects photon pairs emitted from a PDC source and uses a polarized beam splitter (PBS) to separate two polarization modes. She detects one of the two modes with her detector (DA) as a trigger, modulates the polarization of the other mode by a polarization controller (PC) and sends it to Bob. On Bob's side, he chooses his basis by a PC and performs a measurement by his detectors (DB_0 and DB_1).

As shown in FIG. 1, a PDC source generates two modes of photons, which can be separated by a polarized beam splitter (PBS). One mode goes to Alice's own detector (DA in FIG. 1) as the triggering signal and the other mode is used as a triggered single photon state for the QKD. When Alice's detector (DA) clicks, we call it a *trigger*. We divide the detection events on Bob's side into two groups depending on whether Alice gets a trigger or not: triggering detection events and non-triggering detection events.

Note that Alice can use either a threshold detector or a photon-number resolving detector (DA in FIG. 1). She only needs to know the number of photons in the trigger mode. So only one detector is sufficient on Alice's side. Due to the high channel losses, without Eve's interference, Bob is highly likely to receive a vacuum or single photon state. Thus it is sufficient for Bob to use threshold detectors. Threshold single photon detectors can only tell whether there a click or not, but not the photon numbers. Bob needs to identify polarizations of incoming photons. Here we assume Alice encodes qubit information in photon polarizations.

In real experiments, there are two types of PDC sources. In triggering PDC QKD, both of these two types can be used. Here we assume Alice uses type-II PDC source. The Hamiltonian of the type-II PDC process in the triggering setup shown in FIG. 1 can be written as [39]

$$H = i\chi a^\dagger b^\dagger + h.c. \tag{1}$$

where $h.c.$ means Hermitian conjugate and χ is a coupling constant which depends on the crystal nonlinearity and the amplitude of the pump beam. The operators $a^\dagger$, $b^\dagger$ and a, b are the creation and annihilation operators of two modes with different polarizations.

The state coming from a triggering PDC source, with a Hamiltonian of Eq. (1), can be written as [39]

$$|\Psi\rangle = (\cosh\chi)^{-1}\sum_{n=0}^{\infty}(\tanh\chi)^n|n,n\rangle. \tag{2}$$

Here we assume the state is single-mode. The expected photon pair number is given by $\mu = \sinh^2\chi$. The probability to get an n-photon-pair is

$$P(n) = \frac{\mu^n}{(1+\mu)^{n+1}}. \tag{3}$$

Here we assume that the PDC source always sends out photon pairs. That is, the photon number of mode a and b are always the same.

There is a nonzero probability for the PDC source to emit more than one photon pairs in one pulse. Thus, Alice may send out multi photon states after she encodes basis and key information by her polarization controller (PC). This is the reason why the triggering PDC QKD suffers from PNS attacks.

Let us compare triggering PDC QKD and entanglement PDC QKD implementations. For the setup of entanglement PDC QKD, one can refer to Ref. [33]. In the triggering PDC

QKD Alice actively encodes the key information, while in the entanglement PDC QKD Alice measures the polarization of one mode of PDC source directly. The advantage of the triggering PDC QKD here is that it does not rely on the polarization correlations between two modes of the PDC source. It only requires photon-pair generation of the source, which means entanglement between photon pairs are not important for triggering PDC QKD. However, in entanglement PDC QKD implementation, the entanglement between two modes has to be well maintained for QKD transmission. We notice that maintaining entanglement in real experiments is a highly non-trivial task [50].

III. MODEL

Lütkenhaus has already studied the model of triggering PDC QKD [8] with threshold detectors. His model is similar to the one of the coherent state QKD, except for a different photon number distribution. For the model of the coherent state QKD, one can refer to Ref. [8, 20]. For the model of entanglement PDC QKD, one can refer to Ref. [33].

A. Photon number channel model

Here we will use the photon number channel model [19]: Alice and Bob have infinite number of channels. For channel i, Alice uses i-photon states (Fock states) to carry the qubit information, with $i = 0, 1, 2 \cdots$. The ith channel corresponds to the case when Alice's photon source emits an i-photon state. Thus, the probability for Alice to use the ith channel is determined by the photon source. For example, in coherent state QKD, the probability for Alice using the different channels follows a Poisson distribution. For the details of the photon number channel model, one can refer to Ref. [20].

We define the yield Y_i to be the probability for Bob to get a detection event conditioned on Alice using the ith channel. As discussed in Section II, we assume that Bob uses a threshold detector. The yield is given by

$$Y_i = 1 - (1 - Y_{0B})(1 - \eta)^i, \tag{4}$$

where Y_{0B} is the background count rate of Bob's detection system, and η is the overall detection probability for Bob, which takes into account the channel transmission efficiency, the coupling efficiency, the detector efficiency and the other losses in Bob's box.

The error rate when Alice uses ith channel is given by

$$e_i Y_i = e_d Y_i + (e_0 - e_d) Y_{0B} \tag{5}$$

where $e_0 = 1/2$ is the error rate of background counts, e_d is the intrinsic detector error rate on Bob's side (e.g., due to misalignment) and Y_i is given by Eq. (4). Here, we neglect the case where both background counts and true signal click since η and Y_{0B} are small. We remark that Eqs. (4) and (5) are true for both triggered and non-triggered cases.

B. On Alice's side

In the triggering PDC QKD, Alice may use either a threshold detector or a photon-number resolving detector. Define an *N-photon-resolving* detector to be a detector that can tell 0, 1, $\cdots$, N photons of incoming signal. For a threshold detector, we have $N = 1$, which can only tell there are photons presenting or not. Given an incoming i-photon state, the probability for Alice's detector to indicate a j-photon state is $\eta_{j|i}$, with $\sum_{j=0}^{j=N} \eta_{j|i} = 1$ for all $i = 0, 1, \cdots$. In general, $\eta_{j|i}$'s are real numbers in [0,1]. We define a j-photon trigger for the case that Alice's detector indicates a j-photon state.

For a triggered PDC photon source, as given in Eq. (2), the probability for Alice's detector to indicate a j-photon detection is

$$P_{Aj} = \sum_{i=0}^{\infty} \frac{\mu^i}{(1+\mu)^{i+1}} \eta_{j|i}. \tag{6}$$

With the assumption that the PDC source always emits photon pairs, the probability (gain) for Alice getting a j-photon detection and Bob getting a detection is

$$\begin{aligned} Q_{\mu,j} &= \sum_{i=0}^{\infty} Q_{i,j} \\ &= \sum_{i=0}^{\infty} \frac{\mu^i}{(1+\mu)^{i+1}} \eta_{j|i} Y_i, \end{aligned} \tag{7}$$

where the yield Y_i is given in Eq. (4). The quantum bit error rate (QBER) conditioned on Alice's j-photon detection, similar to Eq. (7), is given by

$$\begin{aligned} E_{\mu,j} Q_{\mu,j} &= \sum_{i=0}^{\infty} Q_{i,j} e_i \\ &= \sum_{i=0}^{\infty} \frac{\mu^i}{(1+\mu)^{i+1}} \eta_{j|i} Y_i e_i. \end{aligned} \tag{8}$$

where the error rate e_i is given in Eq. (5).

One observation is that in the triggering PDC QKD setup, shown in FIG. 1, the quantities Y_i and e_i are independent of Alice's measurement outcome j. This is based on the single-mode PDC source assumption described in Eq. (1) in Section II. Therefore, in Section IV, we can apply the decoy state idea.

C. Threshold detector

Here we will discuss a special case that Alice uses a threshold detector. That is,

$$\begin{aligned} \eta_{0|i} &= (1-Y_{0A})(1-\eta_A)^i \\ &\simeq (1-\eta_A)^i \\ \eta_{1|i} &= 1-\eta_{0|i} \\ \eta_{j|i} &= 0, \qquad \forall j \geq 2, \end{aligned} \tag{9}$$

where Y_{0A} and η_A are the background count rate and the detector efficiency on Alice's side. The approximation is due to the fact that normally we have $\eta_A \gg Y_{0A}$. That is, we neglect the background contributions on Alice's side.

According to Eqs. (7) and (8), without Eve's interference, the gains and QBER's of triggered ($j=1$) and non-triggered ($j=0$) detections are given by

$$\begin{aligned} Q_{\mu,0} &= \frac{1}{1+\eta_A\mu} - \frac{1-Y_{0B}}{1+(\eta_A+\eta-\eta_A\eta)\mu} \\ Q_{\mu,1} &= 1 - \frac{1}{1+\eta_A\mu} - \frac{1-Y_{0B}}{1+\eta\mu} + \frac{1-Y_{0B}}{1+(\eta_A+\eta-\eta_A\eta)\mu} \\ E_{\mu,0}Q_{\mu,0} &= e_dQ_{\mu|0} + \frac{(e_0-e_d)Y_{0B}}{1+\eta_A\mu} \\ E_{\mu,1}Q_{\mu,1} &= e_dQ_{\mu|1} + \frac{(e_0-e_d)\eta_A\mu Y_{0B}}{1+\eta_A\mu}. \end{aligned} \tag{10}$$

Without Eve's interference, the gains and error rates of the single photon state in two detections are given by

$$\begin{aligned} Q_{1,0} &= \frac{\mu(1-\eta_A)}{(1+\mu)^2}Y_1 \\ Q_{1,1} &= \frac{\mu\eta_A}{(1+\mu)^2}Y_1 \\ e_1Y_1 &= e_dY_1 + (e_0-e_d)Y_{0B} \end{aligned} \tag{11}$$

where Y_1 and e_1 are given in Eq. (4) and (5), respectively.

D. Perfect photon-number resolving detector

Here we will discuss the case that Alice uses a perfect photon-number resolving detector, which can faithfully tell the number of photons in the incoming signal. That is, $\eta_{j|i} = \delta_{ij}$. Thus the gains and QBER's are given by, from Eqs. (7) and (8),

$$\begin{aligned} Q_{\mu,i} = Q_{i,i} &= \frac{\mu^i}{(1+\mu)^{i+1}} Y_i \\ E_{\mu,i} Q_{\mu,i} = e_i Q_{i,i} &= \frac{\mu^i}{(1+\mu)^{i+1}} e_i Y_i, \end{aligned} \tag{12}$$

from where one can directly infer the gains and error rates of i-photon state, $Q_{i,j} = Q_{i,i}\delta_{i,j}$.

IV. POST-PROCESSING

In the following discussion, we will focus on BB84 protocol [1]. Due to PNS attacks [9, 14, 15], only vacuum states and single photon states are secure for BB84 protocol, which may not be true for other protocols, such as SARG04 [40].

Similar to the coherent state QKD, we can apply GLLP [12] security analysis to the triggering PDC QKD. First, Alice and Bob perform error correction, after which they will share an identical key. Then, they perform privacy amplification to different types of qubits separately. Since here we assume only vacuum states and single photon states are secure for BB84 protocol, the key generation rate is given by [19, 41, 42]

$$R \geq q\{-f(E_\mu) Q_\mu H_2(E_\mu) + Q_1[1 - H_2(e_1)] + Q_0\}, \tag{13}$$

where q is the basis reconciliation factor (1/2 for the BB84 protocol due to the fact that half of the time Alice and Bob disagree with the bases, and if one uses the efficient BB84 protocol [43], $q \approx 1$), the subscript μ denotes for the expected photon pair number, Q_μ and E_μ are the overall gain and QBER, Q_1 and e_1 are the gain and error rate of single photon states, Q_0 is the gain of vacuum states, $f(x)$ is the bi-direction error correction efficiency (see, for example, [44]) as a function of the error rate (normally $f(x) \geq 1$ with the Shannon limit $f(x) = 1$) and $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary entropy function.

All the classical data measured can be grouped according to Alice's detection events, $j = 0, 1, \cdots, N$. Then we can apply the GLLP idea [12, 45] to each group. The final key

generation rate will be given by summing over contributions from all groups,

$$R = \sum_{j=0}^{N} R_j. \tag{14}$$

In each case j, one can apply Eq.(23),

$$R_j \geq q\{-f(E_{\mu,j})Q_{\mu,j}H_2(E_{\mu,j}) + Q_{1,j}[1 - H_2(e_1)] + Q_{0,j}\}, \tag{15}$$

where $Q_{0,j}$ and $Q_{1,j}$ are the first and second terms in the right hand side of Eq. (7). Here the error rate of single photon state e_1 is independent of j, see the observation in the end of Section III B. We note that the key generation rate from all j-photon trigger detections should be non-negative. If any of them contributes a negative key generation rate, we should assign 0 to it. In this case, Alice and Bob can just discard that type of detections. Based on this observation, we can further simplify Eq. (14). Given Alice detects more than one photons, the probability of emitting single photon state in Bob's arm is small [51]. As we mentioned in the beginning of this section, only single photon state can contribute positively to the final key rate. Thus we can focus on the case $j = 0, 1$.

$$R = R_0 + R_1, \tag{16}$$

where R_0 and R_1 are given in Eq. (15). Again, both R_0 and R_1 should be non-negative, otherwise should be assigned 0.

In Eq. (15), the gain $Q_{\mu,j}$ and the QBER $E_{\mu,j}$, given in Eqs. (7) and (8), can be measured or tested from QKD experiments directly. In this section, we will discuss various ways to estimate $Q_{0,j}$, $Q_{1,j}$, and e_1. We assume that the PDC photon source and detector characteristics are fixed and known to Alice. That is, μ, the photon number distribution in Eq. (3) and η_A are fixed and known.

A. Non-decoy states with threshold detectors

Here we assume that Alice uses a threshold detector. Thus, Alice only has two measurement outcomes, $j = 0, 1$. One simple way to estimate $Q_{0,j}$, $Q_{1,j}$, and e_1 is by assuming that all losses and errors come from the single photon states. This is because Eve can in principle perform PNS attacks on the multi-photon states. The gain and error rate of the single

photon states in triggered ($j = 1$) and non-triggered ($j = 0$) detections can be bounded by

$$\begin{aligned} Q_{1,0} &\geq Q_{\mu,0} - \sum_{i=2}^{\infty} \frac{\mu^i}{(1+\mu)^{i+1}} \eta_{0|i} \\ &= Q_{\mu,0} - \frac{(1-\eta_A)^2 \mu^2}{(1+\eta_A \mu)(1+\mu)^2} \\ Q_{1,1} &\geq Q_{\mu,1} - \frac{\eta_A (2-\eta_A+\mu)\mu^2}{(1+\eta_A \mu)(1+\mu)^2} \\ e_{1,0} &\geq \frac{E_{\mu,0} Q_{\mu,0}}{Q_{1,0}} \\ e_{1,1} &\geq \frac{E_{\mu,1} Q_{\mu,1}}{Q_{1,1}} \end{aligned} \tag{17}$$

where η_A is the efficiency of Alice's detector. The gain Q_μ and the QBER E_μ, given in Eqs. (7) and (8), can be measured or tested from QKD experiments directly. In the following simulations, we will use Eqs. (10). Since we assume all errors come from the single photon states, one should take the lower bound of the vacuum contribution to be $Q_{0,j} = 0$.

B. Infinite active decoy state with threshold detectors

To do privacy amplification, Alice and Bob need to bound $Q_{0,j}$, $Q_{1,j}$, and e_1 for Eq. (15). From Eq. (7), we know that to bound $Q_{0,j}$ and $Q_{1,j}$, Alice and Bob need to estimate Y_1.

Decoy state method provide a good way to estimate Y_1 and e_1 [16, 19]. The essential idea is that instead of considering each linear equation of Y_1 and e_1 in the form of Eqs. (7) and (8) separately, Alice and Bob consider all the linear equations simultaneously.

Let us imagine that Alice and Bob obtain an infinite number of linear equations in the form of Eqs. (7) and (8), e.g., they use an infinite number of intensities μ. In principle, Alice and Bob can solve the equations to get Y_1 and e_1 accurately. Mathematically, the problem is solvable. The intuition is that the contributions from higher order terms of Y_i and e_i decrease exponentially in Eqs. (7) and (8). For the case coherent state QKD, one or two decoy states are proven to be sufficient [20]. Shortly, we will see that one decoy state is sufficient for triggering PDC QKD.

We remark that the key underlying assumption of the decoy state method is [19]

$$\begin{aligned} Y_i(decoy) &= Y_i(signal) \\ e_i(decoy) &= e_i(signal). \end{aligned} \tag{18}$$

In another word, Eve sets the same values of Y_i and e_i for decoy and signal states. This can be guaranteed by the assumption that Eve cannot distinguish decoy and signal states.

In Appendix A, we will show that the optimal μ for the infinite decoy state case is in the order of 1, $\mu = O(1)$, which yields final key rate $R = O(\eta)$. On the other hand, the optimal μ for non-decoy case is $\mu = O(\eta)$, which yields final key rate $R = O(\eta^2)$. Therefore, we expect the decoy state QKD to become a standard technique not only in the coherent state QKD, but also in QKD with triggering PDC sources.

There are various ways to apply the decoy state idea to the triggering PDC QKD [34, 35, 36]. Here we consider the upper bound (infinite decoy state case) of all possible decoy protocols of triggering PDC QKD with threshold detectors: triggering PDC+infinite decoy method [19]. In the infinite decoy state method, Alice and Bob perform infinite number of decoy states by choosing different intensities of the PDC source, μ. Then they can solve the linear equations in the form of Eqs. (7) and (8) to estimate Y_1 and e_1 accurately. So they can calculate each $Q_{0,j}$, $Q_{1,j}$, and e_1 accurately. In the simulation, we will use Eqs. (10) and (11) directly.

C. Weak active decoy state with threshold detectors

Here we assume that Alice and Bob use threshold detectors and focus on triggered detection events. Alice uses another intensity ν, say by attenuating pumping laser, for the weak decoy state. Wang, Wang and Guo have proposed a practical decoy method for triggering PDC QKD [36], which is essentially applying vacuum+weak decoy state method [20]. Note that for triggered detection events, the vacuum contribution can be negligible since $\eta_A \gg Y_{0A}$. Thus there is no need to estimate the vacuum contribution here. So Alice and Bob only need to perform weak decoy state instead of vacuum+weak decoy states. In this case, only one weak decoy state is sufficient.

Bounds of Y_1 and e_1 are given by $\mu^2(1+\nu)^3 \times Q_{\nu,1} - \nu^2(1+\mu)^3 \times Q_{\mu,1}$ in Eq. (7) and Eq. (8)

$$\begin{aligned} Y_1 &\geq \frac{1}{\eta_A(\mu-\nu)}[\frac{\mu}{\nu}(1+\nu)^3 Q_{\nu|1} - \frac{\nu}{\mu}(1+\mu)^3 Q_{\mu|1}] \\ e_1 &\leq \min\{\frac{(1+\mu)^2}{\mu}\frac{E_{\mu,1}Q_{\mu,1}}{\eta_A Y_1}, \frac{(1+\nu)^2}{\nu}\frac{E_{\nu,1}Q_{\nu,1}}{\eta_A Y_1}\} \end{aligned} \tag{19}$$

where ν is the expected photon pair number of the weak decoy state and η_A is the efficiency

of Alice's threshold detector.

It is not hard to show that when $\nu \to 0$, Eq. (19) approaches the infinite case, Eqs. (10) and (11), described in the previous subsection.

D. Passive decoy state

Recently, Mauerer and Silberhorn proposed a passive decoy state scheme, in which photon-number resolving detectors are required [34]. Let us recap the heuristic idea of the original passive decoy state scheme briefly here. As discussed in the Section III, Alice and Bob eventually get different detection events grouped by triggers on Alice's side. The key idea proposed by Mauerer and Silberhorn is that Alice and Bob manually combine the $\{j\}$-trigger detection events to get the decoy states with different photon number statistics and then follows regular decoy state scheme.

Here we want to point out that the "combination" step is unnecessary. In general, each detection event group with j-trigger has a different photon number statistics on photon source arm. Thus, what Alice and Bob need to do is treating all $\{j\}$-trigger detection events statistics separately. Furthermore, photon-number resolving detectors are not necessary in passive decoys state scheme. Our new generalized passive decoy state scheme is as follows.

1. Alice uses a PDC source as her triggered photon source. She detects one of the modes from her PDC source as trigger and encode key information into another mode. Due to the detector Alice uses, she will get different trigger events: $j = 0, 1, \cdots$. When she uses a threshold detector, she will only get $j = 0, 1$.

2. As usual BB84 protocol, Bob measures signals in two different bases. Alice and Bob perform basis reconciliation.

3. Alice announces her trigger detection results for each pulse: j. Bob group his detection events by the information j. For each j, they calculate the gain $Q_{\mu,j}$ and test the QBER $E_{\mu,j}$.

   Mathematically, they will obtain a set of linear equations in the form of Eqs. (7) and (8). Notice that the setup parameters, μ and $\eta_{j|i}$'s, are known to Alice and Bob. Thus, they can estimate Y_1 and e_1 by considering Eqs. (7) and (8).

4. Apply post-processing according to Eq. (16).

We remark that the scheme is called *passive* because Alice does not actively select decoy states. Instead, she determines the decoy states by measuring the trigger mode. Later, we will show that this is one advantage of using triggering PDC source for QKD. Actually, in this case, there is no strict definitions of decoy states and signal states. In the original decoy state method [20], decoy states are only used to estimate Y_1 and e_1 and the key is always generated from signal states [52]. In triggering PDC QKD case, both the triggered $j = 0$ and non-triggered $j = 1$ detection events may have positive contribution to the final key generation.

E. Passive decoy state with threshold detectors

Here we will review the decoy protocol proposed by Adachi, Yamamoto, Koashi and Imoto [35] as a special case of the passive decoy state protocol. The AYKI protocol is interesting in practice since it doesn't involve any hardware change to implement decoy state.

Both Alice and Bob use threshold detectors, thus they have two types of detection events, triggered ($j = 1$) and non-triggered ($j = 0$). Secure keys can be generated from both types of detection events. Following the passive decoy state method procedure described in the previous subsection, Alice and Bob can estimate Y_1 and e_1 by considering the statistics of triggered and non-triggered detection events together. This is conceptually similar to one decoy state idea [20].

By solving two linear equations of Eq. (7) with $j = 0, 1$, $[1 - (1 - \eta_A)^2] \times Q_{\mu,0} - (1 - \eta_A)^2 \times Q_{\mu,1}$, one can get

$$Y_1 \geq Y_1^L \equiv \frac{(1+\mu)^2}{\mu}[\frac{2-\eta_A}{1-\eta_A}(Q_{\mu,0} - Q_{0,0}) - \frac{1-\eta_A}{\eta_A}Q_{\mu,1}] \tag{20}$$

where $Q_{0,0}$ is the vacuum state contribution in non-triggered detection events. One need to minimize the key rate of Eq. (16) for $Q_{0,0}$ with the constraint of Eq. (8). We note that this result is essentially the Eq. (14) given in Ref. [35]. We can see that when η_A is close to 1 or μ is small, after neglecting $Q_{\mu,0}$ (background counts), the lower bound Y_1^L is tight (approaches the real value of Y_1, see Eq. (4)),

$$\lim_{\eta_A \to 1} Y_1^L = \lim_{\mu \to 0} Y_1^L = \eta. \tag{21}$$

By neglecting the vacuum state contribution for triggered detection events, $Q_{0,1} = 0$, e_1 can be simply estimated by

$$e_1 \leq \frac{E_{\mu,1} Q_{\mu,1}}{Q_{1,1}}. \tag{22}$$

To get the lower bound of Y_1 in Eq. (20), one has to estimate the background contribution $Q_{0,0}$ as well. One simple bound of $Q_{0,0}$ is $0 \leq Q_{0,0} e_0 \leq E_{\mu,0} Q_{\mu,0}$ from Eq. (8), where $e_0 = 1/2$.

We note that the key rate calculated by substituting Eqs. (20) and (22) into Eq. (16) is not optimal. To get a tighter key rate bound, one can numerically lower bound Eq. (16) directly given the measurement results, Eq. (11).

F. With a perfect photon-number resolving detector

Here we discuss a special case that Alice uses a perfect photon-number resolving detector, discussed in Section III D. Now that Alice knows the exact photon number of the source, Alice and Bob only need to focus the post-processing on the single photon state detection events. In this case, the BB84 protocol is implemented by single photon states only. Thus, they can directly apply Shor and Preskill's formula [5, 33]

$$R \geq q Q_1 [1 - f(e_1) H_2(e_1) - H_2(e_1)]. \tag{23}$$

Later from the simulation, shown in Fig. 2, we can see that a perfect photon-number resolving detector does not improve the QKD performance dramatically comparing to the threshold detector case.

G. A few remarks

From the analysis of optimal μ in Appendix A, one can see that the key rate for the case without decoy states quadratically depends on the channel loss, $R = O(\eta^2)$, while for the case with decoy states, $R = O(\eta)$. This result is consistent with prior work in comparing the cases of coherent state QKD with and without decoy states [19].

In the decoy state security proof [19], the key assumption is that the decoy state and signal state should satisfy Eq. (18). This is guaranteed by the assumption that Eve cannot distinguish decoy and signal states. However, in the active decoy state method, Alice may introduce side information that can distinguish decoy and signal states when she actively

prepares decoy and signal states. For example, an attenuator on Alice's side, used to prepare different intensities for signal and decoy states, may introduce different frequency shifts for signal and decoy states [24]. In general, it is hard to verify the assumption that Eve cannot distinguish decoy and signal states in real active decoy state experiments.

In the passive decoy state scheme, decoy and signal states are passively determined by Alice's measurement outcome. Alice does not use an extra component (like in active decoy state method) to prepare decoy states. This reduces the possibility of side information leakage. By passively choosing decoy states, Alice prepares same states on Bob's arm [53]. In fact, Alice can measure trigger signals after Bob finishes his measurements. Thus, to Eve's point of view, the states transmitted through the channel is independent of Alice's measurement results (j). Therefore, in principle, Eve cannot distinguish the decoy and signal states in the passive decoy state QKD.

This is the main advantage to use passive decoy state methods. Note that for coherent state QKD, one can only use active decoy state idea.

V. SIMULATION

In this section, we will compare the passive decoy state with a perfect number resolving detector and four QKD implementations with threshold detectors: non-decoy, infinite decoy, weak active decoy and AYKI (passive decoy state).

We deduce experimental parameters from a recent PDC experiment [38], which are listed in TABLE I. In the following simulations, we will use $q = 1/2$ and $f(E_\mu) = 1.22$ in Eq. (15). We notice that with the slightly modified experiment setup, a coherent state QKD with decoy states has been implemented [38]. Thus, it is reasonable to use this experiment setup to simulate the five QKD implementations.

In the simulation, for fair comparison, we always assume Bob uses the same detection setup (with threshold detectors).

A. Without statistical fluctuations

In the first simulation, we consider the case that Alice and Bob performs an infinitely long QKD (no statistical fluctuations). In this case the weak active decoy state protocol

Frequency	Wavelength	η_A	η_{Bob}	e_d	Y_{0B}
249MHz	710 nm	14.5%	14.5%	1.5%	6.024×10^{-6}

TABLE I: List of parameters from 144 km PDC experiment [38]. Here η_A and η_{Bob} are the detection efficiencies in Alice and Bob's detection system, not including the optical channel loss. e_d is the intrinsic detector error rate. Y_{0B} is the background count rate of Bob's detection system (for example, if Bob has two detectors, then Y_{0B} will be the sum of two detectors' background count rates). The transmission efficiency η in Eq. (4) is given by η_{Bob} plus the channel loss.

will approach the infinite decoy case [20]. We assume that Alice is able to adjust μ (the brightness of the PDC source) in the regime of $[0, 1]$ arbitrarily. In the simulation, we numerically optimize μ for each of the four implementation protocols: non-decoy, infinite decoy, AYKI and the case with a perfect number resolving detector. The simulation result is shown in FIG. 2.

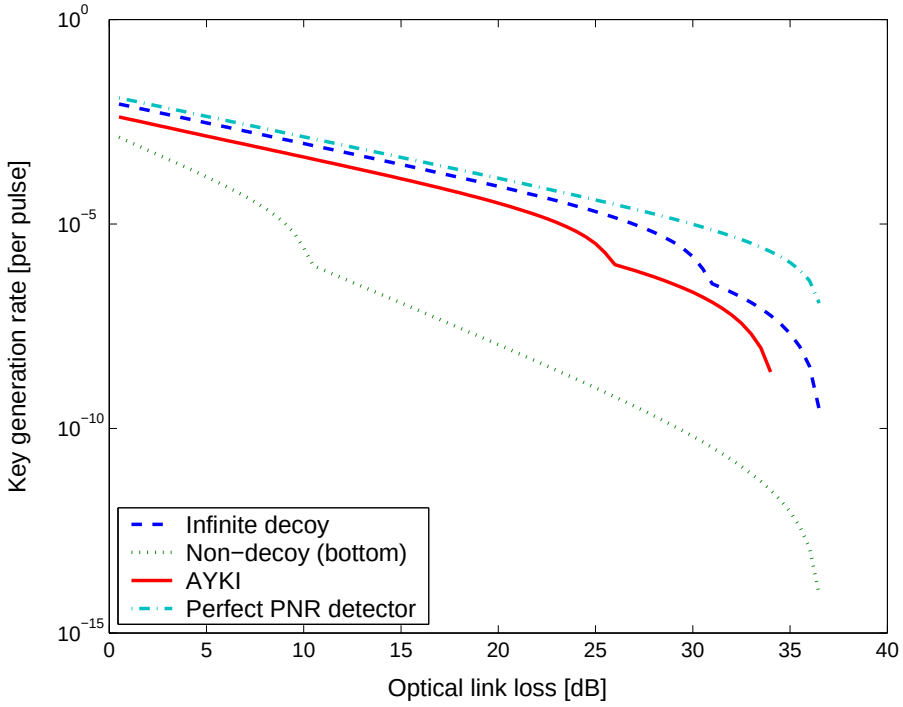

FIG. 2: Plot of the key generation rate in terms of the optical loss, comparing four schemes without considering statistical fluctuations: non-decoy, infinite decoy, AYKI and the case with a perfect number resolving detector. Here we use $q = 1/2$ and $f(E_\mu) = 1.22$. We numerically optimize μ for each curve, see Appendix A for more discussions. Simulation parameters are listed in Table I.

From FIG. 2, we have the following remarks.

1. In Appendix A, instead of numerically optimizing μ as done for Fig. (2), we qualitatively investigate the optimal μ for triggering PDC QKD with and without decoy states. The simulation result is consistent with the qualitative conclusion $R = O(\eta)$ for the case with decoy state and $R = O(\eta^2)$ for the case without decoy state.

2. The space between the solid line and dashed line in FIG. 2 indicates the room left for improvement by other decoy protocols with threshold detectors after AYKI protocol is implemented. We can see that, in a large optical link loss regime, the performances of AYKI and the infinite decoy are close. For instance, the AYKI protocol yields around 50% of the key rate of the infinite decoy state protocol when the channel loss is within 20dB.

3. By comparing AYKI and the case with a perfect photon-number resolving detector, we can see that even with a perfect photon-number resolving detector on Alice's side, the key rate is not improved dramatically in a large optical loss regime.

4. The non-decoy protocol is better than AYKI in the regime close to maximal secure distances. This is because we use the bounds of Eqs. (20) and (22) for AYKI curve. In reality, Alice and Bob can use the bound of Eq. (17) directly in this regime.

5. There is a bump in each curve. This is due to the fact that in the key generation rate formula Eq. (16), the non-triggered detection events have no contribution to the final secure key after the bump.

6. At the point of loss=0 dB, the key rates of four cases (from top to bottom) are 1.21×10^{-2}, 8.6×10^{-3}, 4.2×10^{-3} and 1.3×10^{-3}.

7. At the point of loss=0 dB, the numerical results for optimal μ for four cases (from top to bottom) are: 1, 0.52, 0.194, 0.0589. The optimal μ for the case with a perfect threshold detector is always 1, which is reasonable since $\mu = 1$ maximizes the single photon state probability. In Appendix A, we show that the optimal μ's for the infinite decoy and AYKI case are relatively stable in a large optical loss regime. The optimal μ for the no decoy state case decreases with channel loss.

8. We remark that the real μ used in the experiment [38] is $\mu = 0.0265$. In general, it is experimentally hard to increase the brightness (μ) of a PDC source.

9. All of the four cases can tolerate similar optical losses.

B. With statistical fluctuations

In a real experiment, the key length is always finite. Alice and Bob should consider statistical fluctuations. As pointed in Ref. [20], statistical fluctuation analysis is a complicated problem in decoy state QKD.

Similar to the analysis in Ref. [20], we assume a few conditions:

1. Alice knows the exact value of average photon pair number μ, which is a fixed number during key transmission.

2. The distribution of photon number, Eq. (3), does not fluctuate.

3. Assume the QKD transmission is part of an infinite length experiment.

Here we focus on the three cases with threshold detectors: infinite decoy, weak decoy and AYKI. We assume that the data size is 6×10^9 pulses of Alice's pumping laser. The simulation result is shown in FIG. 3. From the simulation result, we have the following observations.

1. Similar to the case without fluctuation analysis, in a large optical link loss regime, the performances of AYKI and the infinite decoy are close.

2. At the point of loss=0 dB, the key rates of the three cases from top to bottom are 8.6×10^{-3} (infinite), 5.0×10^{-3} (weak) and 4.7×10^{-3} (AYKI).

3. The maximal tolerable secure optical losses for three cases are rather similar: 37dB (infinite), 32.5dB (AYKI), 32dB (weak).

4. The AYKI protocol yields a higher key rate than weak decoy state protocol when the loss is greater than 16 dB. AYKI is less affected by statistical fluctuations than the weak decoy state because in AYKI, Alice does not need to sacrifice extra pulses for decoy states.

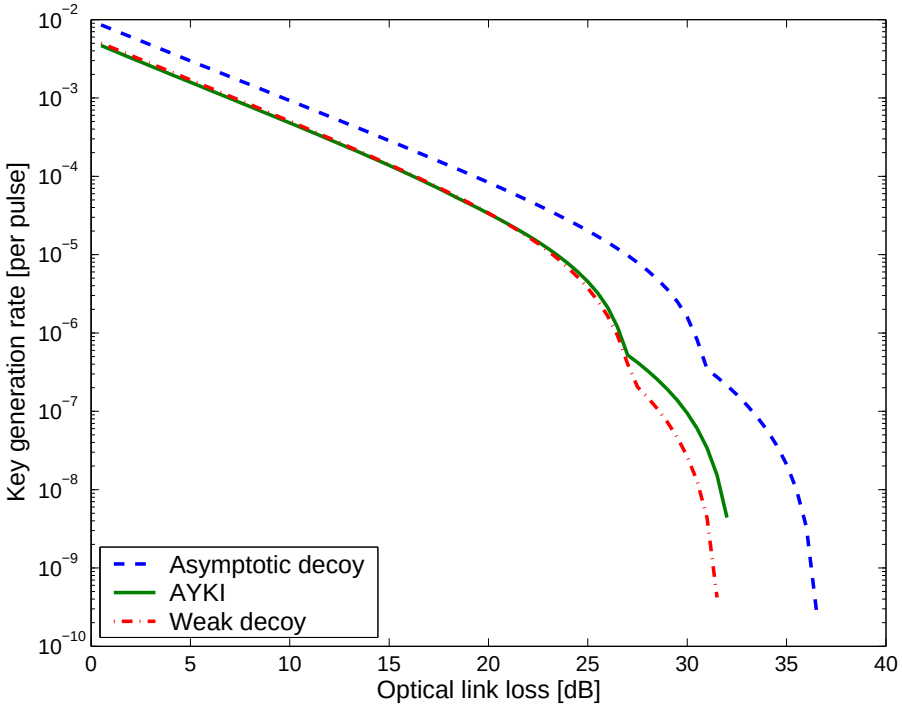

FIG. 3: Plot of the key generation rate in terms of the optical loss, comparing three cases with threshold detectors after considering statistical fluctuations: infinite decoy, weak active decoy and AYKI. We numerically optimize μ for each curve. Here we use $q = 1/2$ and $f(E_\mu) = 1.22$. In the weak decoy state case, we assume Alice can randomly attenuate her PDC source intensity. Simulation parameters are listed in Table I. The data size is 6×10^9 pumping laser pulses on Alice's side.

In Section IV G, we pointed out that from a practical security point of view, the passive decoy state method has an advantage over active decoy state methods. Also, AYKI method does not require any additional hardware change to implement decoy state, while in the weak decoy state case, Alice needs to add an attenuator to create decoy states. Now, from the simulation result, we can see that AYKI and weak active decoy state method yields similar QKD performance. Thus, our conclusion is that one should just use AYKI method instead of the weak decoy state method.

VI. CONCLUSION

By investigating the optimal photon source intensity, we find that the triggering PDC QKD setup with decoy states is able to achieve a key rate that linearly depends on the channel transmittance, comparing to the quadratic dependence for the case without decoy states. Therefore, we expect the decoy state QKD to become a standard technique not only in the coherent state QKD, but also in QKD with triggering PDC sources.

On the practical side, we generalize the passive decoy state idea. The generalized passive decoy state idea can be applied to cases where either threshold detectors or photon number resolving detectors are used. The decoy protocol proposed by Adachi, Yamamoto, Koashi and Imoto (AYKI) can be treated as a special case of the generalized passive decoy state method. Comparing to the active (regular) decoy state methods, the passive one opens less possibility for Eve to distinguish decoy and signal states, which is a key underlying assumption in the security proof of decoy state QKD. From this sense, the passive decoy state method is more secure than the active decoy state methods in practice.

By simulating a recent PDC experiment, we compare various practical decoy state protocols with the infinite decoy protocol. We also compare the cases using threshold detectors and photon-number resolving detectors. Our simulation result shows that with the AYKI protocol, one can achieve a key generation rate that is close to the theoretical limit of infinite decoy protocol. Furthermore, our simulation result suggests that a photon-number resolving detector has little room to improve the QKD performance, comparing to the case using threshold detectors.

We also consider the statistical fluctuations. We compare infinite decoy protocol, weak active decoy state method and AYKI protocol. The simulation result shows that the weak active decoy state method and AYKI protocol yield very close QKD performance. In a large optical loss regime, the AYKI protocol can achieve a performance that is close to the infinite decoy case. Since the AYKI protocol requires no hardware changes for triggering PDC QKD, we conclude that AYKI method is a good protocol for triggering PDC QKD experiments.

Although our analysis is focused on the QKD with PDC sources, we emphasize that it can also be applied to other QKD setups with triggered single photon sources.

VII. ACKNOWLEDGMENTS

We thank C.-H. F. Fung, W. Mauerer, A. M. Steinberg and G. Weihs for enlightening discussions. In the simulation part, we thank H. Hübel for confirming the parameters we deduced from their experiments. This work has been supported by CFI, CIFAR, CIPI, Connaught, CRC, MITACS, NSERC, OIT, PREA, QuantumWorks and the University of Toronto. X. Ma gratefully acknowledges Chinese Government Award for Outstanding Self-financed Students Abroad and the Lachlan Gilchrist Fellowship.

APPENDIX A: OPTIMAL μ

The optimal μ for the coherent state QKD with and without decoy states has already been studied [20]. Here instead of numerically optimizing μ as done for Fig. (2), we qualitatively investigate the optimal μ for the triggering PDC QKD with and without decoy states. Here we are interested in the case that Alice uses a threshold detector.

1. Without decoy states

Let us begin with the optimal μ of the case without decoy states. Here we will apply GLLP [12] security analysis. As shown in Ref. [46], GLLP and Lütkenhaus's [8] security analyses achieve similar performances for the coherent state QKD. Intuitively, we should get a similar optimal μ as given in Ref. [8], $\mu \approx \eta/2$.

From Eq. (10), we can see that the gain $Q_{\mu,j}$ $(j = 0, 1)$ is in the order of $\mu\eta$. To keep $Q_{1,0}$ or $Q_{1,1}$ in Eq. (17) positive, μ should be in the order of η. By assuming μ, η and Y_{0B} are small, we can simplify Eq. (10)

$$\begin{aligned} Q_{\mu,0} + Q_{\mu,1} &\approx \eta\mu \\ E_{\mu,0} \approx E_{\mu,0} &\approx e_d \\ Q^L_{1,0} + Q^L_{1,1} &\approx \eta\mu - \mu^2 \\ e^U_1 &\approx \frac{\eta e_d}{\eta - \mu} \end{aligned} \tag{A1}$$

where $Q^L_{1,0} + Q^L_{1,1}$ is the lower bound of $Q_{1,0} + Q_{1,1}$ and e^U_1 is the upper bound of e_1 from Eq. (17). Since the error rates from triggered $(j = 1)$ and non-triggered $(j = 0)$ detection

events are the same, the key generation rate given by Eq. (23) can be simplified to

$$\begin{aligned} R &\geq q\{-f(E_\mu)Q_\mu H_2(E_\mu) + Q_1[1 - H_2(e_1)] + Q_0\} \\ &\approx q\{-f(e_d)\eta\mu H_2(e_d) + (\eta\mu - \mu^2)[1 - H_2(\frac{\eta e_d}{\eta - \mu})]\} \end{aligned} \tag{A2}$$

By taking derivative of R, the optimal $\mu \equiv x\eta$ satisfies

$$-f(e_d)H_2(e_d) + 1 - 2x + e_d \log_2 \frac{e_d}{1-x} + (1 - e_d - 2x)\log_2(1 - \frac{e_d}{1-x}) = 0. \tag{A3}$$

Here if set $e_d = 0$, then we get $x = 1/2$ which is compatible with Lükenthaus' result [8]. We note that $x = 1/2$ essentially maximize the probability of single photon source $Q^L_{1,0} + Q^L_{1,1}$ in Eq. (A1). More precisely, we can solve Eq. (A3) numerically, see FIG. 4.

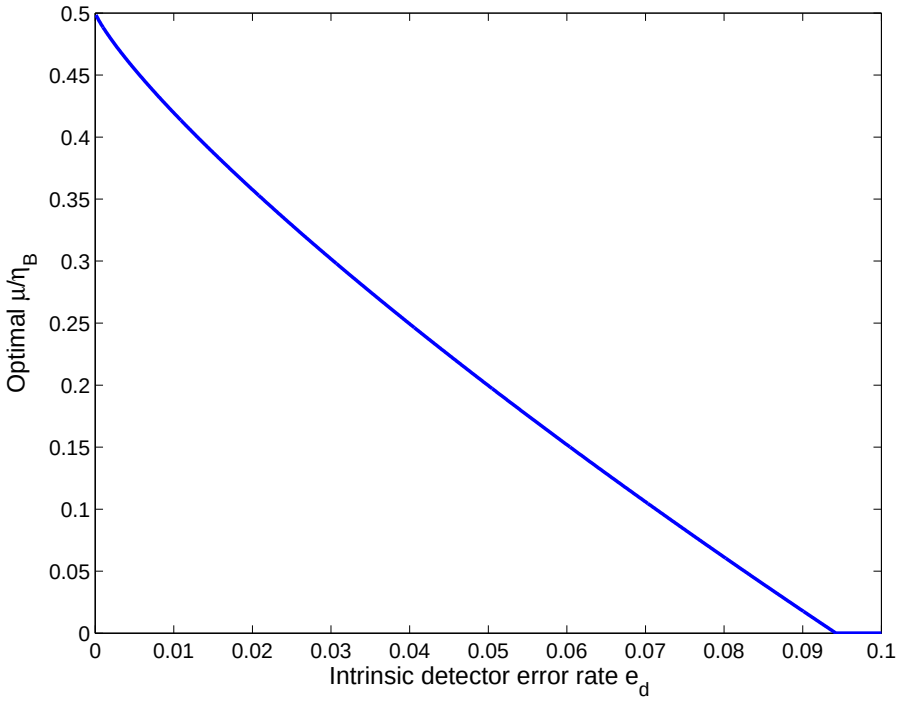

FIG. 4: Plot of the optimal μ in terms of e_d for triggering PDC+non-decoy. Here we use $f(e_d) = 1.22$ since the error rate is less 10% [44].

From FIG. 4, we can see that the optimal μ for triggering PDC+non-decoy is $\mu = O(\eta)$, which will lead the final key generation rate $R = O(\eta^2)$.

2. With decoy states

With decoy states, Alice and Bob can estimate Q_1 and e_1 better. Here we consider the infinite decoy state case with threshold detectors. Under the assumption that η and Y_{0B} are

small, we can simplify Eqs. (10) and (11),

$$\begin{aligned} Q_{\mu,0} + Q_{\mu,1} &\approx \eta\mu \\ E_{\mu,0} &\approx E_{\mu,0} \approx e_d \\ Q_{1,0} + Q_{1,1} &\approx \frac{\eta\mu}{(1+\mu)^2} \\ e_1 &\approx e_d \end{aligned} \tag{A4}$$

With these approximations, the key generation rate given in Eq. (23) can be simplified to

$$R \approx q\{-f(e_d)\eta\mu H_2(e_d) + \frac{\eta\mu}{(1+\mu)^2}[1 - H_2(e_d)]\}. \tag{A5}$$

The optimal μ satisfies

$$\frac{1-\mu}{(1+\mu)^3} = \frac{f(e_d)H_2(e_d)}{1 - H_2(e_d)} \tag{A6}$$

Here if set $e_d = 0$, then we get $\mu = 1$ with which the probability to get a single photon state is maximized. The numerical result of Eq. (A6) is shown in FIG. 5.

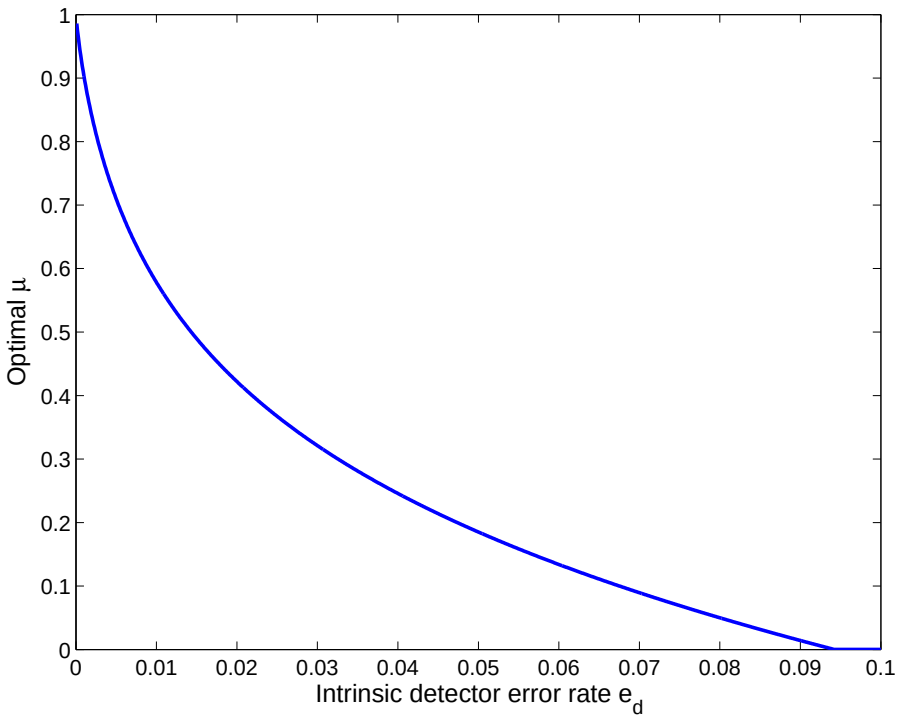

FIG. 5: Plot of the optimal μ in terms of e_d for the triggering PDC+infinite decoy. Here we use$f(e_d) = 1.22$.

From FIG. 5, similar to the case coherent state QKD with decoy states [20], one can see

that the optimal μ is independent of channel loss η for the infinite decoy state case with threshold detectors, i.e., $\mu = O(1)$, which will lead the final key generation rate $R = O(\eta)$.

3. Numerical checking

Now we would like to numerically compare the optimal μ with and without decoy states by simulating a recent PDC experiment [38], with parameters listed in Table I. In the simulation, we numerically optimize μ for the key rate given by Eq. (16) for the non-decoy and infinite decoy methods. For this particular setup, the optimal μ is shown in Figure 6.

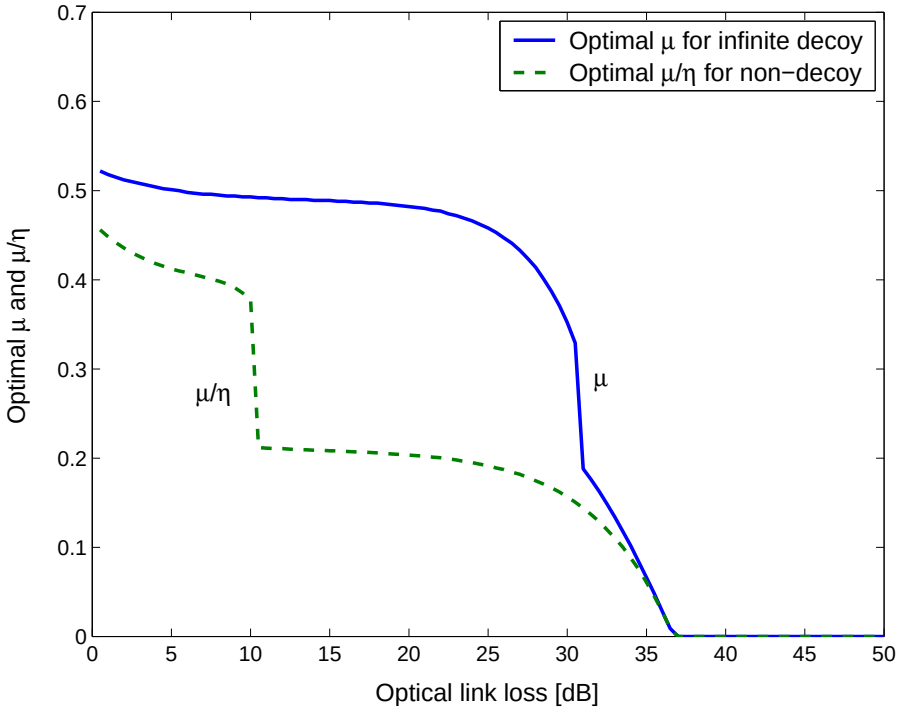

FIG. 6: Plot of the optimal μ in terms of optical loss for triggering PDC+non-decoy and triggering PDC+infinite-decoy. Here we use $q = 1/2$ and $f(E_\mu) = 1.22$. Simulation parameters are listed in Table I.

From the figure we can see that the optimal μ for the non-decoy case is in the order of η, while the optimal μ for the infinite-decoy case is in the order of 1. This is consistent with

the results of the analysis in the two previous subsections.

---

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, Bangalore, India, 1984), pp. 175–179.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] D. Mayers, Journal of the ACM **48**, 351406 (2001).

[4] H.-K. Lo and H.-F. Chau, Science **283**, 2050 (1999).

[5] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[6] M. Koashi, J. Phys. Conf. Ser. **36**, 98 (2006).

[7] D. Mayers and A. Yao, in *FOCS, 39th Annual Symposium on Foundations of Computer Science* (IEEE, Computer Society Press, Los Alamitos, 1998), p. 503.

[8] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).

[9] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[10] H. Inamori, N. Lütkenhaus, and D. Mayers, Eur. Phys. J. D **41**, 599 (2007).

[11] M. Koashi and J. Preskill, Phys. Rev. Lett. **90**, 057902 (2003).

[12] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Information and Computation **4**, 325 (2004).

[13] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. A. Smolin, Journal of Cryptology **5**, 3 (1992).

[14] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).

[15] N. Lütkenhaus and M. Jahma, New Journal of Physics **4**, 44.1 (2002).

[16] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[17] H.-K. Lo, in *Proc. of IEEE ISIT* (IEEE, 2004), p. 137.

[18] X. Ma, arXiv: quant-ph/0503057 (2004).

[19] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[20] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[21] J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt, ArXiv.org:quant-ph/0503002 (2005).

[22] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[23] X.-B. Wang, Phys. Rev. A **72**, 012322 (2005).

[24] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).

[25] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, in *Proc. of IEEE ISIT* (IEEE, 2006), p. 2094.

[26] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Phys. Rev. Lett. **98**, 010503 (2007).

[27] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, et al., Phys. Rev. Lett. **98**, 010504 (2007).

[28] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. **98**, 010505 (2007).

[29] Z. L. Yuan, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **90**, 011118 (2007).

[30] M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004).

[31] K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe, arXiv:quant-ph/0607082 (2006).

[32] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).

[33] X. Ma, C.-H. F. Fung, and H.-K. Lo, Phys. Rev. A **76**, 012307 (2007).

[34] W. Mauerer and C. Silberhorn, Phys. Rev. A **75**, 050305(R) (2007).

[35] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. Lett. **99**, 180503 (2007).

[36] Q. Wang, X.-B. Wang, and G.-C. Guo, Phys. Rev. A **75**, 012312 (2007).

[37] Q. Wang, X.-B. Wang, G. Björk, and A. Karlsson, Europhysics Letters **79**, 40001 (2007).

[38] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, et al., Nature Physics **3**, 481 (2007).

[39] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer, Berlin, 1994).

[40] V. Scarani, G. R. A. Acin, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

[41] H.-K. Lo, Quantum Information and Computation **5**, 413 (2005).

[42] M. Koashi, arXiv:quant-ph/0609180 (2006).

[43] H.-K. Lo, H.-F. Chau, and M. Ardehali, Journal of Cryptology **18**, 133 (2005).

[44] G. Brassard and L. Salvail, in *Advances in Cryptology EUROCRYPT '93*, edited by G. Goos and J. Hartmanis (Springer-Verlag, Berlin, 1993).

[45] X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo, Phys. Rev. A **74**, 032330 (2006).

[46] X. Ma, Phys. Rev. A **74**, 052325 (2006).

[47] See Section II for the definition of a trigger.

[48] In a non-triggered detection event, Bob gets a detection but Alice doesn't get a trigger.

[49] Sometimes it is called heralded single photon source.

[50] We thank A. M. Steinberg for enlightening discussions.

[51] In Section II, we assume that Alice's PDC source always sends out photon pairs. Given that Alice detects more than one photons on the triggering arm, a single photon state presents on the other arm only when there is a dark count in Alice's detector. Normally, we can assume that the detector efficiency is much higher than the dark count probability on Alice's side. Thus, we neglect probability of a single photon state with a multi photon trigger.

[52] In the coherent state QKD, there is an optimal μ for a setup. To maximize the final key rate, Alice and Bob should publicly compare all detection results from decoy states.

[53] Strictly speaking, there is one underlying assumption: the PDC source is single-mode.